

The Payment Card Industry (PCI) Data Security Standards (DSS) v1.2 Requirements:

Using Server Isolation and Encryption
as a Regulatory Compliance Solution and
IT Best Practice



Introduction

This paper addresses the challenge of regulatory compliance requirements driven by PCI DSS version 1.2. As this paper suggests, the best response is to take a risk-based approach that builds on a base of server isolation and end-to-end encryption to meet both existing requirements and expected changes to PCI DSS.

What is PCI DSS?

The Payment Card Industry (PCI) Data Security Standards (DSS) were developed to assist companies that process credit or debit card payments in protecting customer data from unauthorized exposure and use. These companies are undergoing examinations and certifications by card associations, including Visa and MasterCard, to determine their compliance with PCI DSS. Failure to meet PCI requirements may lead to the loss of the right to process credit and debit card payments, financial penalties and long-term damage to customer trust and brand equity.

The core of the PCI DSS is a group of principles and accompanying requirements that consolidated five credit card company requirements in December 2004. Minor revisions and clarifications were developed in v1.1 released September 2006. On October 1, 2008, v1.2 was released to further clarify requirements, offer more flexibility and address evolving threats and vulnerabilities. PCI DSS v1.1 requirements will sunset on December 31, 2008.

PCI DSS v1.2¹ contains the same number of requirements (12) for compliance that are organized into the previous 6 logically related groups, which are called “control objectives.” According to the PCI DSS Frequently Asked Questions³, “...v1.2 does not introduce any new, major requirements” and was primarily issued to add clarity to v1.1 standards.

A Closer Look at the Changes in PCI DSS v1.2

Strong Access Control

PCI DSS v 1.2 has new advice on the use of “internal firewalls, routers with strong access control” and other technologies to restrict access to critical customer data related to credit card

1 https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

2 https://www.pcisecuritystandards.org/pdfs/pci_dss_summary_of_changes_faqs_v1-2.pdf

processing³. Deploying internal firewalls and routers is a way to segment a flat corporate network to limit access to critical data. Companies have also deployed virtual local area networks (VLANs) and Network Admission Control (NAC) solutions to segment networks for access control. The key point is that PCI DSS regulations recommend not a single solution but rather layers of security to restrict access to cardholder data.

According to a recent Network World article⁴ “one of the biggest topics of debate at last month’s PCI Council meeting was how to determine what ‘network segmentation means’ since the standard is aimed at trying to devise technical methods to cordon off where credit cards are stored so that PCI compliance assessment can be focused on specific parts of a merchant’s network involved with cardholder data.” An IT best practice is to move the security solution closer to the data. One method is the use of an internal firewall. The benefit of this strategy is that the portion of the network where cardholder data exists is segmented from the rest of the network, which limits the scope of the PCI audit and the complexity of proving compliance to that smaller surface area.

Firewalls were designed to protect the perimeter of a corporate network. Using them to segment an internal corporate network may not be efficient or cost effective for many companies. And, the fact that PCI DSS allows for other technologies and includes a section on compensating controls to protect customer data should lead companies to seek layers of security.

Companies should strive to identify areas where card data is located and perform an analysis on the risk of a database or network breach. Then, consider layers of security that can be implemented closer to where the data resides. Companies are using a software-based server isolation security solution that resides on hosts where cardholder information is stored. Moving the solution closer to the data and isolating the system will reduce the attack surface. Providing walls of separation between the critical cardholder data and other corporate data imposes strong access control and limits the scope and complexity of a PCI DSS audit.

Encryption

The PCI Council did not make a change to the rules regarding encrypting cardholder data. Encrypting data is a key guidance of PCI DSS v1.2 related to using cryptographic methods to protect information traveling over open, public networks. Data sent in the clear on the

³ “Credit-card security standard issued after much debate”, Ellen Messmer, Network World, October 1, 2008

⁴ Ibid

Internet is an easy target for data thieves. Companies typically use virtual private network (VPN) encryption methods to protect data in a “tunnel” over the public because it is secure and cost effective.

Most company internal network data traffic over wired networks is sent in the clear. For that reason, data thieves have shifted their focus on targeting corporate network data. For example, at the Hannaford US supermarket chain over 4.2 million customer credit and debit card numbers were compromised. Thieves gained access to “data in motion” via purchase transactions at hundreds of retail stores. And, new network breaches by companies like Hannaford who claim to be PCI compliant will likely drive the Council to revisit the encryption of all cardholder data traffic on a company’s internal network, possibly suggesting end-to-end encryption of that traffic.

Any company that wants to avoid a breach and associated negative effects should consider encrypting cardholder data in motion on their corporate networks. Employing stronger end-to-end encryption will move security closer to the data, add an extra layer of security and mitigate the risk of a data breach. And, the PCI Council indicated that new guidelines on end-to-end encryption may be released in 2009.⁵

Virtualization Security

Unfortunately, PCI DSS v1.2 does not address the vulnerabilities associated with virtualization security. However, it was a topic discussion and new guidelines on securing virtualized environments are expected in 2009. According to Gartner, 60% of virtual machines will be less secure than their physical counterparts through 2009. Virtual machines (VMs) themselves are no less secure than physical systems, but organizations often apply different procedures to their deployment and management. And, server virtualization architecture introduces new vulnerabilities and challenges if not properly addressed.

Any legacy security solutions such as firewalls, VLANs, intrusion prevention systems (IPS), etc., rely on associating an IP address to a location and making a security decision based on that location. In a virtualized environment, IP addresses often change as virtual machines are created, retired or migrated from one physical host to another, causing issues in traditional protection mechanisms.

⁵ Ibid

Virtual machines are easily created from previously existing images, often introducing large numbers of VMs that are not properly maintained or are based on images with known vulnerabilities. Also, server virtualization introduces the concept of a “soft switch” to allow for VMs to communicate with each other inside a single host. Special tools are required to monitor and protect these communications and solution options are limited.

Anyone running server virtualization technology should analyze whether their security solution is sufficient for protecting cardholder data on VMs. Companies are deploying agent-based security software to each virtual machine that provides both server isolation to control access to VMs storing customer data combined with encryption to mitigate the risk of the loss or exposure of critical data in motion. This strategy of adding layers of security functions to protect cardholder data – the intent of PCI DSS v1.2.

Choosing the Best PCI DSS Compliance Strategy

PCI DSS v1.2 access control and encryption requirements are primarily focused on securing the network perimeter and protecting data in motion over public networks. By strictly adhering to these guidelines, companies that process credit and debit card transactions may be vulnerable to internal network attacks. Furthermore, in deploying server virtualization on a corporate network increases the risk of an attack because it adds additional complexity to controlling access to customer data. Adding virtualization to a compliant network could lead to non-compliance if those VMs are not properly secured.

The PCI Council is expected to update PCI DSS soon. According to a recent Network World article, “The council indicated that next year it will focus on new guidelines for end-to-end encryption, payment machines and virtualization.”⁶ Historically, new standards revisions are delivered every two years. The fact that new guidelines for encryption and virtualization security will be addressed within a year suggests that companies should explore adding extra layers of security to mitigate the risk of an internal network data breach.

⁶ Ibid

Using Apani® EpiForce® as an IT PCI DSS Compliance Best Practice

As part of a total solution for PCI DSS v1.2, Apani EpiForce can restrict access to cardholder data inside the network perimeter with logical security zoning and policy based encryption of data in motion. Logical security zones isolate systems that store, process or transmit cardholder data into PCI security zones for an extra layer of security. Customer credit card information that is transmitted within the security zone or over a network within a company location or data can be encrypted for extra security.

For companies unable to encrypt credit card data at rest, compensating controls may be considered. Compensating controls restrict access to cardholder data with added security zones and policy based encryption of data in motion. EpiForce provides a solution to block the connectivity of unauthorized users or devices and is an excellent option for achieving PCI compensating controls.

The next section will discuss specific PCI DSS v1.2 requirements related to access control and encryption and how EpiForce server isolation and encryption of data in motion is an IT best practice in achieving PCI DSS compliance. Other PCI DSS requirements unrelated to a solution like EpiForce have been omitted from this discussion. If you have any questions on EpiForce or would like a free PCI best practices security assessment, please contact Apani at Americas +1 (866) 638-5625 or Europe +44 (0) 207-887-6060.

PCI DSS Requirements and Security Assessment Procedures Version 1.2

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

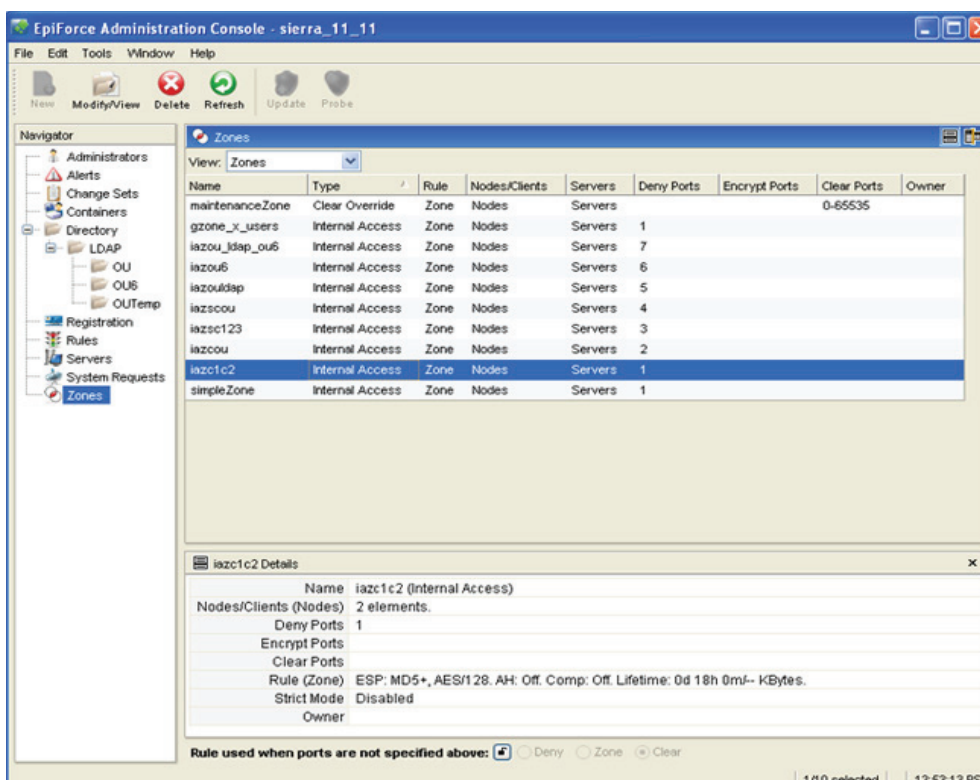
Summary: This requirement is focused on deploying and managing firewall appliances. There are procedures for establishing firewalls, rules to restrict outside, direct access to the cardholder data environment and direction to install firewall software on portable systems that company employees use to access the internet.

How EpiForce Can Help: Firewalls are ideal for protecting a corporate network from unauthorized intrusions from the internet or public network and for that reason they are commonly used.

However, once an approved outside system is granted access to the corporate network, a skilled user could use unapproved methods, such as a packet sniffer to improperly access sensitive or confidential information such as cardholder data, and usernames and passwords. Additionally, IT managers commonly make configuration errors that create “holes” in firewalls that allow unauthorized access to data contained on hosts attached to the internal network.

EpiForce delivers server isolation to provide access control to systems storing cardholder data. It is complimentary technology to the firewall requirements in this section by providing additional security behind the firewalls guarding IT assets inside the LAN. Through a centralized EpiForce Admin Console located virtually anywhere on the network, the solution can create a PCI security zone that includes systems storing credit and debit card information. EpiForce software agents installed on the systems also combine access control and isolation with policy-based encryption of communications in the PCI security zone or between zones. EpiForce Agents are designed to work on mobile clients in changing environments, including dynamic addressing (DHCP) and Network Address Translation (NAT), in conjunction with personal firewall software.

Firewalls have been used to establish PCI security zones inside the perimeter and are commonly called “internal firewalls”. However, this method may not be efficient to deploy or easy to manage for most companies. Changes to firewall rules to accommodate new security policies create additional management complexity. And, EpiForce security policies are easily controlled through a central management utility, rather than dealing with the complexity of firewall rule changes.



EpiForce Admin Console used to set security policies

Server virtualization technology is being installed by many companies who need to maintain PCI compliance. Since cardholder data is located on these systems, it's important to properly secure them. For these companies deploying server virtualization, EpiForce is an ideal security solution. Once an EpiForce Agent is installed on a virtual machine (VM), the VM can be assigned to a PCI security zone regardless of where the host or VM is located. Multiple VMs in that host or other hosts in different locations can be assigned to PCI security zones, to deliver efficient use of IT assets. Security policy deployed by EpiForce remains persistent, regardless of the physical location of a server or client. For example, a VM could be located in a host in a company's California office and be moved to a different host anywhere on the corporate network. When a machine is moved, the security policy goes with the machine and does not require any policy changes or administrative action. When EpiForce VM is deployed, agents also automatically reconfigure security policy when a VM is restarted, avoiding a security gap.

EpiForce manages both virtual and physical IT assets, regardless of platform or physical location. Deploying a virtual-only security solution requires companies to take a silo approach to security, increasing management complexity. EpiForce alleviates this concern by managing both virtual and physical servers and endpoints from a centralized console.

Protect Cardholder Data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Summary: This requirement strives to prevent data breaches by nefarious individuals who target network vulnerabilities. It directs that companies encrypt customer data that passes over open, public networks such as the Internet through the use of strong security protocols. Strong cryptography and security protocols such as SSL/TLS or IPsec are provided as examples. The requirement is focused on eliminating vulnerabilities found in poorly configured wireless networks and in legacy authentication and encryption protocols. The intent of this requirement is to secure customer data wherever it may be transmitted.

How EpiForce Can Help: When critical customer information is transmitted outside the corporate network, it typically passes through a firewall onto the Internet, through a virtual private networking (VPN) tunnel. Industry standard protocols such as SSL or IPsec are applied using strong encryption to protect the data from the risk of a loss or unauthorized exposure. The internal network is defined as the communication paths found within the company data center or one of its many locations. Unfortunately, credit and debit card information along with usernames and passwords are often transmitted in the clear on a company's internal network making that critical data vulnerable to attack by malicious individuals. Even worse is that much of this data is transferred over RF technology such as WiFi. Even though WiFi offers strong security it is often not used. It can also be hard to setup and is often inconsistent when combined with wired networking. EpiForce offers consistent, centrally managed security across all of these infrastructures,

EpiForce applies policy-based encryption to customer data being transmitted on the company's internal network. EpiForce uses IPsec, a standard security protocol, for authenticated, secure network communications. By encrypting corporate network communications, EpiForce adds an extra layer of security that mitigates the risk of an internal data breach.

EpiForce policy-based encryption is centrally managed through one or more administration consoles, enabling encryption policy for the entire EpiForce deployment to be modified with only a few mouse clicks. Administration can be delegated and workflow enabled for approving and committing policy changes.

Securing virtualized environments adds extra complexity. Communications between virtual machines (VMs) can occur within the same physical host or between hosts in different locations. Furthermore, virtualization technology makes it easy to create new VMs or move established VMs to different hosts. An EpiForce Agent installed on each VM will deliver encrypted communications between VMs in a physical host or different hosts.

Security policy deployed by EpiForce remains persistent, regardless of the physical location of a server or endpoint. When a virtual machine is moved, the security policy goes with the virtual machine and does not require any policy changes or administrative action. When EpiForce VM is deployed, agents also automatically reconfigure security policy when a VM is restarted, avoiding a security gap.

Maintain a Vulnerability Management Program

Requirement 6: Develop and maintain secure systems and applications

Summary: This requirement was created to deter individuals with malicious intent from exploiting systems and application vulnerabilities. Many of these vulnerabilities can be traced to companies not installing current security patches, which expose machines and applications. Once exposed, hackers can gain access to critical customer data. Procedures are encouraged to install updates and participate in alert services. The intent of specific standards such as 6.3.2 “Separate development/test and production environments” and “Separation of duties between development/test and production environments” prevent cardholder data from inadvertently being exposed to those working on development/test environments.

How EpiForce Can Help: Specific standards such as 6.3.2 “Separate development/test and production environments” and “Separation of duties between development/test and production environments” are relevant to a security solution such as EpiForce. EpiForce zoning or host isolation can be used as a mechanism to achieve separate development/test and production environments through logical security zoning. EpiForce lets you segment machines and users on your network in development/test environments, which mitigate the risk of exposing data to unscrupulous individuals.

For companies who want to enjoy the benefits of server virtualization and maintain strong security, EpiForce is an ideal solution. Security policy deployed by EpiForce remains persistent, regardless of the physical location of a server or client. When a server is re-purposed, the

existing security policy travels with the VM and does not require any policy changes or administrative action, unless new policies are warranted. This will prevent unauthorized access to applications or data in a production environment from a user assigned to a development/test environment or visa versa. When EpiForce VM is deployed, agents also automatically reconfigure security policy when a VM is restarted, avoiding a security gap.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

Summary: Companies are directed to employ methods that limit access to cardholder data to those users that require access to that information as part of their job. Examples of those methods include having rights to systems that store cardholder data and allowing multiple users on a single machine to access the protected system depending on their rights to that information.

How EpiForce Can Help: EpiForce can be used to establish a PCI security zone that includes systems where cardholder data is stored. A security policy may be established that allow controlled access to an application on a set of authorized ports. The procedure places a wall around the data on that protected host in the PCI zone.

Relative to “7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities, EpiForce enforces user-based security policy to the protected systems in that zone through an integration with Microsoft Active Directory. This simplifies the process of assigning user rights because once the policies are set in Active Directory, they will be automatically included in the EpiForce security solution. Changes can be easily integrated in EpiForce once they have been set in Active Directory.

In the PCI DSS Requirement 7 section, there are these rules: “7.2 Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed. This access control system must include the following: 7.2.1 Coverage of all system components, 7.2.2 Assignment of privileges to individuals based on job classification and function, and 7.2.3 Default “deny-all” setting”. EpiForce is explicitly designed to meet these requirements. EpiForce supports user-based and host-based security policies. This allows IT managers to restrict access to a host with critical cardholder data based on a user’s authorization. If a user’s job function changes

where they should not have access to that host, a new policy can be created to limit that access. EpiForce Agents can be configured to block all unauthorized network communications by default provided that access controls are based on access to applications or services.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Summary: There must be an audit trail for tracking and monitoring access to network resources and cardholder data. This information is critical to maintaining cardholder data security. “Logging mechanisms” and the ability to monitor “user activities” are important in meeting this requirement. Companies must link access to sensitive or confidential data, have secured, and automated audit trails down to the event level.

How EpiForce Can Help: EpiForce is an excellent solution for meeting many of the sub-requirements of this section⁷, which is detailed in the following table:⁸

PCI DSS Requirements	Apani EpiForce
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	All administrator actions in EpiForce are independently logged and special privileges are required to view the logs. Alterations and deletions can be detected.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	
10.2.2 All actions taken by any individual with root or administrative privileges	All administrator actions in EpiForce are independently logged and special privileges are required to view the logs. Alterations and deletions can be detected.
10.2.3 Access to all audit trails	EpiForce Database Server logs access.
10.2.4 Invalid logical access attempts	EpiForce Agents log dropped communications, such as when an attacker attempts to communicate on a blocked or secure port. This includes IPsec negotiation failures. Failed EpiForce administrator login attempts are also logged.
10.2.5 Use of identification and authentication mechanisms	EpiForce Agents log negotiations, which includes the identity of the remote Agent from its certificate. EpiForce administrator logins are also logged.

⁷ Requirements that are unrelated to the EpiForce security solution have been omitted.

⁸ For EpiForce to log activities, an administrator must initiate a network communication via a network application. EpiForce is not able to record administrator activities within an authorized application nor can EpiForce record what administrators do locally on the host.

PCI DSS Requirements	Apani EpiForce
10.2.6 Initialization of the audit logs	EpiForce Agents, Admin Servers, etc. write startup information in their audit logs each time the Agent is restarted, or when logs are rolled over.
10.2.7 Creation and deletion of system-level objects	All administrator activities are independently logged, including when Agents are created or deleted in the EpiForce domain.
10.3 Record at least the following audit trail entries for all system components for each event:	
10.3.1 User identification	Administrator access is available in the current product. User-based policy will be included in the next release.
10.3.2 Type of event	Agents log IPSec negotiations, many other communications events. Admin Consoles log all administrator activities.
10.3.3 Date and time	Yes, date and time are recorded by EpiForce.
10.3.4 Success or failure indication	Yes, success and failure indications are provided by EpiForce.
10.3.5 Origination of event	Yes, the origination of events is recorded by EpiForce. For Agent communications, the Agents at both ends log events, including source and destination information.
10.3.6 Identity or name of affected data, system component, or resource	Yes. Agents are uniquely identified in the EpiForce domain and they record that information as they establish operational communications with each other.
10.4 Synchronize all critical system clocks and times.	Partially. Clocks must be manually synchronized, or you can use a trusted time server. EpiForce will drop communications (and log them) if clocks are seriously mismatched.
10.5 Secure audit trails so they cannot be altered.	
10.5.1 Limit viewing of audit trails to those with a job-related need.	Administrator actions: Yes - special privileges required. EpiForce Agent logs: No, to permit internal user support for communications issues.
10.5.2 Protect audit trail files from unauthorized modifications.	Yes. Audit trail files are protected from unauthorized modifications.

The Apani Solution: EpiForce

Designed to isolate servers, VMs, endpoints and business-critical data within the corporate network, Apani EpiForce VM is an ideal solution for flexible access management and is trusted by the world's largest financial service organizations. More than 60 Fortune 100 companies use Apani's core technology, which was created with a grant from the National Security Agency to protect communications in the event of a nuclear war.

By isolating systems into logical security zones and strictly controlling who has access to these security zones, EpiForce is a superior alternative to deploying, configuring and managing firewalls and VLANs.

Due to its software-based architecture, EpiForce is easier to manage, more flexible, quicker to deploy and has an overall lower total cost of ownership. Leveraging digital certificates to authenticate users and systems, EpiForce strengthens authentication in virtual environments.

EpiForce is easy to deploy, highly scalable and transparent to infrastructure, applications and users, and it will meet the needs of any large corporation.

Visit www.apani.com/epiforce-trial to request a free 30-day full featured EpiForce VM trial. Or Call Americas +1 (866) 638-5625 Europe +44 (0) 207-887-6060